DETAILED ACTION

1. Currently pending claims are 1, 3, 5, 7, 8 and 10 – 17.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

Claim Objections

3. Claim 17 is objected to because of the following informalities: "makes a computer perform which detects" should be replaced with "makes a computer perform detecting". Appropriate correction(s) is (are) required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 1 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claim(s) recite(s) a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claim(s) is/are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The recited method

claim(s) including steps of detecting and performing is (are) broad enough that the claim(s) could be completely performed mentally, verbally or without a machine nor is any transformation apparent. Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 3, 5, 7, 8 and 10 – 17 are rejected under 35 U.S.C. 102(e) as being anticipated by Albert et al. (U.S. Patent 2003/0177389) – This also includes the reference incorporated by reference Freund et al. (U.S. Patent 2003/0055962) – see (Albert: Para [0096]).

As per claim 1 and 5, Albert teaches a method in which a computer acquires particular data through a network, said method comprising steps of:

detecting a first activation instruction to activate a program that connects to the network and sends and receives communications in a state that the already-operating computer is not connected to the network (Albert: Para [0025] Line 1 – 4 / Line 11 – 13: the activation of a program of a computing device and the state which is already-operating but not yet connected to the network must be detected first, so that the requirement to apply a local security policy first can be met in order to subsequently connect the computing device to the network);

performing particular data acquisition processing for acquiring the particular data through the network, when a first activation instruction to activate said program is detected (Albert: Para [0068] Line 12 – 15 and Para [0066] Line 15 – 21: the security policy must be updated first via the network (i.e. only after the updated security policy is applied via the network to the already-connected computer) before the program (e.g., internet browser) can be activated to access the network resource).

thereafter, activating said program whose activation has been instructed (see the same rationale of rejection as above).

As per claim 7 and 16, Albert teaches a network security enhancing system for a computer, comprising:

a means that detects a first activation of a program that connects to a network and sends and receives communications in a state that the already-operating computer is not connected to the network (Albert: Para [0025] Line 1 – 4 / Line 11 – 13: the activation of a program of a computing device and the state which is already-operating but not yet connected to the network must be detected first, so that the requirement to apply a local security policy first can be met in order to subsequently connect the computing device to the network); and

a means that activates processing of updating a security file at activation of a said program after processing of connection to said network and before other processing (Albert: Para [0068] Line 12 – 15 and Para [0066] Line 15 – 21: the security policy must be updated first via the network (i.e. only after the updated security policy is applied via the network to the already-connected computer) before other processing of the program (e.g., internet browser) can be activated to access the network resource).

As per claim 15 and 17, Albert teaches a network security enhancing system for computer, wherein:

a means that detects first activation of a program that connects to the network and sends and receives communications, in a state that an already operating computer is not connected to the network (Albert: Para [0025] Line 1 – 4 / Line 11 – 13: the activation of a program of a computing device and the state which is already-operating but not yet connected to the network must be detected first, so that the requirement to apply a local security policy first can be met in order to subsequently connect the computing device to the network);

a means that activates the processing of updating the security file at activation of said program, after processing of connection to said network and before other processing, activates processing of connecting to the network and processing of updating a security file, and thereafter activates said program that sends and receives communications (Albert: Para [0068] Line 12 – 15 and Para [0066] Line 15 – 21: the security policy must be updated first via the network (i.e. only after the updated security policy is applied via the network to the already-connected computer) before other processing of the program (e.g., internet browser) can be activated to access the network resource);

a means that detects a program that is installed on the computer and connects to a network and sends and receives communications (Albert: Para [0025] Line 1 – 4 / Line 11 – 13: the installation of a program of a computing device which is already-operating but not yet connected to the network can be detected upon the network access / connection attempt so that the requirement to apply a local security policy first can be met in order to subsequently connect the computing device to the network),

a means that detects an activation instruction of a program that connects to said network and sends and receives communications (Albert: Para [0068] Line 12 – 15 and

Para [0066] Line 15 – 21: the activation of a program of a computing device can be detected so that the security policy can be updated first via the network (i.e. only after the updated security policy is applied via the network to the already-connected computer) and then other processing of the program (e.g., internet browser) can be subsequently activated to access the network resource);

a means that activates network connection processing (see the same rationale of rejection as above).

As per claim 3, Albert teaches said particular data acquisition processing is processing of updating a security file (Albert: Para [0068] Line 12 – 15 and Para [0066] Line 15 – 21: the security policy must be updated first via the network (i.e. only after the updated security policy is applied via the network to the already-connected computer) before other processing of the program (e.g., internet browser) can be activated to access the network resource).

As per claim 8, Albert teaches a means that displays a message reporting completion of said processing of updating the security file, after the processing has been completed (Albert: Para [0062] / [0043]: capable to display the result of the operation which includes security policy update).

As per claim 10, Albert teaches said processing of updating the security file is processing of acquiring amendment of a definition file used for an antivirus countermeasure (Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: displaying “the system has detected that you must update your current virus software” – which surely includes the current virus definition file).

As per claim 11, Albert teaches said processing of updating the security file is processing of acquiring a patch file (Freund: Para [0149] and Para [0149] Line 13 – 17: a security patch file applied to a non-compliant computer in order to continue t proceed a particular network connection).

As per claim 12, Albert teaches a means that activates the processing of updating the security file at activating a browser and before displaying a screen (Albert: Para [0025] & Freund: Para [0007], Para [0027] Para [0117] and Para [0149] Line 13 – 17: (a) updating a security policy on the connection to a particular network by (b) using WWW (i.e. web browser) for the connection to a large network (c) updating the security file at activating a browser for connecting to a particular large network and (d) the first screen will not be proceeded for security policy in-compliance – i.e. the remote log-on screen will not be displayed).

As per claim 13, Albert teaches a means that outputs a message requesting activation of the processing of updating the security file, after said program that connects to the network and sends and receives communications connects to the network and before said program starts communication operation (Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: displaying "the system has detected that you must update your current virus software" – which surely includes the current virus definition file) & (Albert: Para [0068] Line 12 – 15 and Para [0066] Line 15 – 21: the activation of a program of a already-connected computing device can be detected so that the security policy can be updated first via the network (i.e. only after the updated security policy is applied via the network to the device) and then other processing of the program (e.g., internet browser) can be subsequently activated to access the network resource).

As per claim 14, Albert teaches a means that outputs a message requesting activation of the processing of updating the security file, at activation of a browser and before displaying a screen (Albert: Para [0025] & Freund: Figure 7 / Element 702 & Para [049], Para [0116], Para [0007], Para [0027] Para [0117] and Para [0149] Line 13 – 17: (a) displaying "the system has detected that you must update your current virus software" – which surely includes the current virus definition file (b) updating a security policy on the connection to a particular network by (c) using WWW (i.e. web browser) for the connection to a large network (d) updating the security file at activating a browser for connecting to a particular large network and (e) the first screen will not be proceeded for security policy in-compliance – i.e. the remote log-on screen will not be displayed).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai E.E. Ph.D
Primary Examiner, Art Unit 2431
02/10/2009